LEARNING MANAGEMENT SYSTEM SECURITY STATEMENT - SUMMARY

INTRODUCTION
Compliance Learning is built on a state-of-the-art world class Learning Management System (LMS) provided by Docebo. The application is hosted on secure cloud on Amazon Web Services (AWS). The following document provides an overview of the architecture and the implementation of several layers of industry security standards to ensure safety, data privacy and confidentiality of our clients.

ARCHITECTURE
The LMS adopts an architecture which involves the duplication of the system’s critical components or functions for redundancy in order to increase their reliability. It incorporates state of the art technology into its different components, and there are multiple layers to provide a secure and reliable system.

SECURITY CONTROLS AND DETAILS
At the routing level, Docebo has implemented both an intrusion detection system and an Intrusion prevention system. These systems monitor and analyze the traffic and identify any possible malicious connection or request. Docebo has also implemented ways to protect the system from cyber-attacks - such as SQL injections, cross-site scripting, and cross site request forgery.

USER ACCESS SECURITY POLICIES
In Compliance Learning, each user is required to verify their login using unique credentials (username and password) in order to access the system, regardless of the user’s role in the system. Anonymous logins are not permitted. The Learning Management System (LMS) allows administrators to configure different levels of complexity in password management, depending on their housekeeping and internal security policies.

SERVER MANAGEMENT SECURITY
Access to the LMS can be limited to connecting only through a secure connection. This ensures that all the data exchanged between LMS servers and the client’s PCs are securely encrypted. The application maintains a secure connection between the server and client by the use of browser cookies and http sessions. No cookies contain any personal data and sessions are maintained in a central repository and timeout once the user is no longer active.

SYSTEM REDUNDANCY AND BACKUP
Docebo’s architecture is built in a redundant (reliable) manner, to properly mitigate and reduce any possible drawbacks caused by outages to specific architectural components, and avoiding taking on a single point of failure. By leveraging the use of state-of-the-art and leading monitoring tools, the system collects all data related to the different systems in a virtual control dashboard. This allows the identification of any warning, outage or performance reduction in the infrastructure. Communication related to outages is kept on an official twitter account dedicated to this communication @DoceboStatus.
UPGRADE AND UPDATE POLICIES
Docebo LMS applies regular maintenance updates, which consists of minor releases that relate to either bug fixes or minor service improvements. These improvements do not affect the LMS’s stability, performance and/or standard behavior, and which can be applied without service interruption. These also do not require a notice time as they are considered part of the standard service housekeeping executed by Docebo on both the standard and Enterprise clusters.

Docebo also provides upgrades by providing new features and are scheduled by giving notice to customers via the appropriate product newsletter or are released on a client request and based on a mutually agreed timeframe.

VULNERABILITY SCANNING
Docebo works with 3rd party company (NOPSEC) that specializes in software vulnerability testing to find and remediate any vulnerabilities that their system might have. NOPSEC performs vulnerability tests on cross site scripting, path traversal, unrestricted file uploads, and SSL cookie set without secure flag. NOPSEC provides and a detailed report on its vulnerability findings, so that Docebo can work to improve any vulnerabilities that may be uncovered.

About this Statement
Compliance Learning and Docebo LMS shall not be liable for any losses or damages suffered arising from reliance being placed upon any of the contents of this document. We reserve the right to amend this statement to reflect updates at any time. Unless otherwise stated, the most recent version shall supersede and replace all previous versions of this privacy and security statement.